International Journal of Innovation in Science and Mathematics
Volume 3, Issue 6, ISSN (Online): 2347–9051

CERT Technologies

Khaled Abdulkareem Alenezi
Department of Computer Science,
International Islamic University of Malaysia,
53100 Jalan Gombak, Kuala Lumpur, Malaysia
Email: alenezi.khaled@yahoo.com

Imad Fakhri Al-Shaikhli
Department of Computer Science,
International Islamic University of Malaysia,
53100 Jalan Gombak, Kuala Lumpur, Malaysia
Email: imadyaseen39@yahoo.com

Lili Marziana Abdullah
Department of Information System,
International Islamic University Malaysia,
53100 Jalan Gombak Kuala Lumpur, Malaysia
Email: lmarziana@iium.edu.my

Mohammad A. AlAhmad
Public Authority of Applied Education and Training,
College of Basic Education, Computer Science Department,
Kuwait City, Kuwait,
Email: malahmads@yahoo.com

***Abstract* – Members of the incident response team should have excellent technical skills, such as system administration, network administration, programming, technical support, malware analysis, and intrusion detection. Moreover, supporting system state and status reporting are associated with enabling automated mechanisms with the hardware or software that report information about the system, including abnormal behavior, intrusion attempts, or any other data that would be useful in detecting an incident, understanding impact, and quickly supporting resolution.**

In order to effectively protect GE and Non-GE entities from cyber-attacks, multiple layers of defenses strategies are needed to combat multiple security issues. The strategy is based on using appropriate security countermeasures across operational, network, and host functionality of GE and Non-GE entities.

Therefore, we proposed four zones segment information architecture for securing the main assets and services of GE and Non-GE entities in Kuwait. In each of these zones specific and unique security focus are addressed.

For each zone of the layered cyber-security systems architecture, technological security elements are presented to help in securing IT assets and services of the organizations. Such a layered cyber-security systems architecture will assist the organizations in creating clear boundaries in order to effectively and practically apply multiple layers of defenses.

***Keywords* – Cert, Technologies.**

I. INTRODUCTION

When a computer security attack on an organization occurs, it is critical for the affected organization to have a fast and effective means of responding. The speed with which the organization can recognize an incident or attack and then successfully analyze it and respond will dramatically limit the damage done and lower the cost of recovery. Careful detection of the nature of the attack or incident can lead to the implementation of effective and widespread preventative measures and the avoidance of similar events. This ability to respond quickly and effectively to a computer security threat is a critical element in providing a secure computing environment [1][15].

As GE and Non-GE entities in Kuwait grow in complexity and are connected to business and external networks, the number of security issues and the associated risks with those issues grow as well. The wide variety of attack vectors that target multiple assets on these organizations can give rise to attacks that can be executed asynchronously, over a long period of time and could target multiple weaknesses and vulnerabilities of the systems environment. A single countermeasure cannot be depended on to mitigate all security issues.

In order to effectively protect GE and Non-GE entities from cyber-attacks, multiple layers of defenses strategies are needed to propagate the risk over an aggregate of security mitigation. The strategy is based on using appropriate security countermeasures across operational, network, and host functionality of GE and Non-GE entities.

Therefore, we proposed four zones segment information architecture for securing the main assets and services of GE and Non-GE entities in Kuwait. In each of these zones specific and unique security focus are addressed. For each zone of the layered cyber-security systems architecture, technological security elements are presented to help in securing IT assets and services of the organizations. Therefore, broad of technological security elements that can be used as operational and technical security controls against cyber-attacks are presented.

Such a layered cyber-security systems architecture will assist the organizations in creating clear boundaries in order to effectively and practically apply multiple layers of defenses.

II. LAYERED SECURITY ARCHITECTURE

A defense-in-depth strategy of multiple layers to combat multiple security issues is required to protect against cyber-attacks for GE and Non-GE entities. The strategy is based on using appropriate security countermeasures across organizations operational, network, and host functionality, and having the aggregate of all security activities provide complete protection over the entire architecture.

Cyber-security is not just about deploying specific technologies to counter certain risks. An effective security program for an organization will depend on its adherence and willingness to accept security as a constant constraint on all cyber activities. Implementing an effective cyber-security strategy will require taking a complete approach and leveraging all of an organization's resources in order to provide effective layers of protection.

Copyright © 2015 IJISM, All right reserved

In order to create a culture for protecting GE and Non-GE entities in Kuwait, the CERT needs to be assembled. The team should include at least one executive level manager for leadership and guidance, security and operations management at the corporate level, and full participation from technical experts. The team need to be trained on the key aspects of cyber-security and be fully aware of the present security challenges and risks that the organizations needs to address in regard to its own assets and services.

In order to create a layered defense, a clear understanding is essential of how all the technology fits together and where all the interconnectivity resides. Dividing the cyber-security systems architecture into zones can assist organizations in creating clear boundaries in order to effectively apply multiple layers of defense. The main factor for creating architectural zones involves understanding how network segmentation can be achieved. Figure 1 shows the proposed four zones segment information architecture for securing the main assets and services of GE and Non-GE entities in Kuwait, which are Exterior Zone, Corporate Zone, Department Zone, and End Device Zone. Each of these zones require a unique security focus to protect against cyber-attacks.

The Exterior Zone represents the area of connectivity of the GE or Non-GE entity to the Internet for a purpose of communication with its branch, client, other organization, or its remote offsite facilities such as cloud storage. This is a point of connectivity that is considered untrusted. Therefore, the exterior zone should has the highest amount of priority as it has the highest variety of risks. The next lower zone of the layered security architecture is called Corporate Zone which represents the area of connectivity inside the organization. The E-mail servers, DNS servers, and IT business system infrastructure components are the typical resources in this zone. A wide variety of risks exist in this zone because of the amount of systems and connectivity to the external zone. Therefore, the corporate zone has a higher precedence than other zones after the external zone. The Department or Unite Zone represents the area of connectivity inside specific unite or department of the organization. This zone includes department network devices and external shared IT-based resources such as peripherals and servers. The Department Zone is the central in the operation of both the end devices and the business requirements of the corporate zone, and the priority of this area is considered to be high. Whereas, the End Device or User Zone represents the area of connectivity per employee inside specific unite or department in the organization. This zone includes employee devices such as Desktops, Laptops, and Smartphones. The device zone is the central to the business processes of the department zone, and the priority of this area is considered to be high.

Based on the proposed layered security architecture, we also should build defensive strategies that secure each of the core zones to offer the constituents more opportunities for protecting critical assets and services.

III. TECHNOLOGICAL DEFENSIVE STRATEGIES

The following categories of technological security products represent common technological elements helpful in securing IT systems and protecting organizations critical assets and services. For each technological security category, a discussion for the types of products in each category is presented.

1. Identification and Authentication Technology

a. Description

Authentication is the means of establishing the validity of this claim. Authorization is the process of defining and maintaining the allowed actions. Identification and authentication establishes the basis for accountability and the combination of all three enables the enforcement of identity-based access control. The user's identity can be authenticated using either something they have like token, password, or fingerprint. The principal forms of authentication include static, dynamic, and multiple factors.

Static. Static authentication reuses a specific authenticator (e.g., static password). This type of authentication only provides protection against attacks in which an imposter cannot obtain the authenticator. The strength of the authentication process is highly dependent on the difficulty of guessing or decrypting the authenticator values and therefore how well they are protected in transit and while stored on the system.

Dynamic. Dynamic authentication uses cryptography or other techniques to create one per-session authenticator. A dynamic authenticator changes with each authentication session between the claimant and verifier.

Multiple Factor. Multiple-factor authentication requires two or more types of authentication techniques. Multiple factor authentication can include both static and dynamic authentication mechanisms. One example is the use of a password along with a smart card token.

On the other hand, authorization mechanisms fall into four major categories:

Local: Local authorization is performed for each application and machine to which a user requires access. The mechanisms of the local operating system and applications are employed to setup and maintain the authorizations for that machine or application.

Network: Authorization is performed at a central, authorization server, providing access to a user's account from one or more workstations on the network. The key here is that the access is to a single user account. If the user requires multiple accounts, then each is a separate authorization and handled in like manner to multiple users.

Single Sign-on: Single sign-on employs a central authorization server to enable a user to authenticate one time in order to achieve access to multiple applications, machines, and domains operating with a variety of authentication mechanisms (for example, a Kerberos implementation within a heterogeneous Windows 2000 and Unix network). The central server contains identifier/authenticator pairs for each domain that the user needs to access and performs an authentication on behalf of the user for each resource that the user is authorized to

Copyright © 2015 IJISM, All right reserved

access. The central server establishes and maintains, as individual actions, the authorizations at each application, machine, or domain that the user is allowed to access.

Single Log-on: Single log-on is similar to single sign-on with the exception that the central server authentication mechanism is the mechanism used by all the applications, machine, and domains with which the user needs to interact. Rather than store identifier/authenticator pairs for each verification, the one-time verification is accepted by all resources as the only verification needed. Additionally, the authorizations are maintained at the central server and the individual applications, machines, and domains query the central location to determine whether a specific access is authorized. Single log-on eliminates the need for authorization at each resource and for individual authentications to each resource.

The following technological support represents the defensive strategies that secure device and department zones to offer the constituents more opportunities for protecting critical assets and services.

b. Technological Support

There are multiple technological products that support authentication and identification functionality. The following ones are the most common:

Security Tokens. Security tokens are used to allow access first to a computer and then to a network. Tokens come in various forms - for example, Personal Computer Memory Card International Association (PCMCIA) cards, flash memory, USB tokens, smart cards, and software.

Certificates. The public key certificate associates a certificate holder's identity with his public key.

Authentication Protocols. These protocols are used to determine who is accessing a resource.

Biometrics. Biometrics are used for physical access control, electronic access control, and monitoring devices. An organization's choice of biometric control depends on the security level required, user acceptance, enrollment speed, and costs incurred [9].

Biometrics technology is used to identify and authenticate an individual based on personal characteristics. Examples of personal characteristics include fingerprints, face, retina, iris, speech, handwriting, hand geometry, and wrist veins.

Biometrics can also be combined with passwords, personal identification numbers (PIN), and cards to further increase accuracy and security.

2. Access Control Technology

a. Description

Access control ensures that only authorized access to resources occurs. Access control helps protect confidentiality, integrity, and availability and supports the principles of legitimate use, least privilege, and separation of duties. Access control simplifies the task of maintaining enterprise network security by reducing the number of paths that attackers might use to penetrate system or network defenses.

Access control systems grant access to information system resources to authorized users, programs, processes, or other systems. Access control may be managed solely by the application, or it may use controls on files. The system may put classes of information into files with different access privileges.

The following technological support represents the defensive strategies that secure corporate and exterior zones to offer the constituents more opportunities for protecting critical assets and services.

b. Technological Support

Access Control Lists. Access control data can reside either in (a) the resource to be protected or (b) a central location based on a model. An example of a data structure used for resource-centric storage of access control information is the Access Control List (ACL). An example of a specification of access control information centrally based on a model is the role-based access control (RBAC) database.

ACLs in routers and other network devices can be used to implement the following forms of access enforcement:

Traffic Filters. Access controls can be enforced effectively at the data packet layer. A filter can block any packet that does not conform to security policy rules. Filters can be assigned to incoming or outgoing traffic. Filtering can be based on source and destination addresses, protocol types, and information from other fields within the packets unless the content is encrypted.

Policy Filters. Policy filters can be used to set up access control policies on routers. Policy filters, which operate to and from routing tables, can be used to specify the routers or networks from which updates will be accepted.

Role-Based Access Control. RBAC has emerged as a promising feature of many database management, security management and network operating system products. The essential advantage of RBAC products is that they allow system administrators to assign individual users into roles. The role identifies users as members of a specific group, based on their capabilities, work requirements, and responsibilities in the organization. Access rights, or security privileges, are then established for each role; a user may belong to multiple roles, which provide the appropriate level of access for their requirements. Thus, the RBAC structure empowers administrators with a tool to regulate which users are given access to certain data or resources, without having to explicitly authorize each user to each resource.

3. Intrusion Detection Technology

a. Description

Intrusion detection is the process of monitoring events occurring in a computer system or network and analyzing them for signs of intrusions, defined as attempts to perform unauthorized actions, or to bypass the security mechanisms of a computer or network. Intrusions are caused by any of the following: attackers who access systems from the Internet, authorized system users who attempt to gain additional privileges for which they are not authorized, and authorized users who misuse the privileges given them. Intrusion detection systems (IDS) are software or hardware products that assist in the intrusion monitoring and analysis process [5].

The implementation of an IDS might be valuable for the following reasons:

- Prevent problem behaviors by increasing risk of

Copyright © 2015 IJISM, All right reserved

discovery and punishment for system intruders

- Detect attacks and other security violations that are not prevented by other security measures
- Detect preambles to attacks (network probes and other tests for existing vulnerabilities)
- Document the existing threat to the organization
- Quality control for security design and administration
- Provide useful information about methods used in intrusions.

There are two different approaches to analyzing events to detect attacks: signature-based detection and anomaly detection. Either or both of the approaches could be used in an IDS product.

Signature-Based Detection. This approach identifies events or sets of events that match with a predefined pattern of events that describe a known attack. These patterns are called signatures. Signatures may include system states, or accessing system areas that have been explicitly identified as off-limits.

Anomaly Detection. Anomaly detection assumes that all intrusive activities deviate from the norm. These tools typically establish a normal activity profile and then maintain a current activity profile of a system. When the two profiles vary by statistically significant amounts, an intrusion attempt is assumed.

The following technological support represents the defensive strategies that secure exterior and corporate zones to offer the constituents more opportunities for protecting critical assets and services.

b. Technological Support

Three common types of IDS products are network based, host based, and application based. Each type of product may optionally offer intrusion prevention capabilities.

Network-Based IDS. These IDSs detect attacks by capturing and analyzing network packets. Listening on a network segment or switch, one network-based IDS can monitor the network traffic affecting multiple hosts that are connected to the network segment.

Network-based IDSs often consist of a set of single-purpose sensors or hosts placed at various points in a network. These units monitor network traffic, performing local analysis of that traffic and reporting attacks to a central management console. Because the sensors are limited to running the IDS, they can be more easily secured against attack. Many of these sensors are designed to run in "stealth" mode, making it more difficult for an attacker to determine their presence and location.

Host-Based IDS. Host-based IDSs operate on information collected from within an individual computer system. This vantage point allows host-based IDSs to determine exactly which processes and user accounts are involved in a particular attack on the OS. Furthermore, unlike network-based IDSs, host-based IDSs can more readily "see" the intended outcome of an attempted attack, because they can directly access and monitor the data files and system processes usually targeted by attacks.

Host-based IDSs normally use information sources of two types: operating system audit trails, and system logs. Operating system audit trails are usually generated at the innermost (kernel) level of the operating system; therefore these trails are more detailed and better protected than system logs. Some host-based IDSs are designed to support a centralized IDS management and reporting infrastructure that can allow a single management console to track many hosts. Others generate messages in formats that are compatible with network management systems.

Application-Based IDS. Application-based IDSs are a special subset of host-based IDSs that analyze the events transpiring within a software application. The most common information sources used by application-based IDSs are the application's transaction log files.

The ability to interface with the application directly, with significant domain or application-specific knowledge included in the analysis engine, allows application-based IDSs to detect suspicious behavior due to authorized users attempting to exceed their authorization. This is because such problems are more likely to appear in the interaction among the user, the data, and the application.

Intrusion Prevention. Intrusion detection systems often have intrusion prevention capabilities. This means that not only can they detect an intrusive activity, but they can also attempt to stop the activity, ideally before it reaches its targets. Intrusion prevention is much more valuable than intrusion detection because intrusion detection simply observes events without making any effort to stop them. Unfortunately, intrusion prevention can also cause operational issues because if the detection of incidents is not accurate, then it may block legitimate activities that are incorrectly classified as malicious. Any organization that wants to utilize intrusion prevention should pay particular attention to detection accuracy when selecting a product.

Another consideration involving intrusion prevention is architecture-related. IDS products may be simply monitoring activity, or they may actually be "in-line", which means that activity must pass through them. Examples include a network-based IDS that is integrated with a firewall and a host-based IDS that is integrated into the kernel of the operating system. An in-line intrusion detection system has the ability to block all detected attacks. If an IDS product is not in-line, its ability to block attacks may be limited.

4. Firewall Technology

a. Description

Firewalls are devices or systems that control the flow of network traffic between networks or between a host and a network. A firewall acts as a protective barrier because it is the single point through which communications pass. Internal information that is being sent can be forced to pass through a firewall as it leaves a network or host. Incoming data can enter only through the firewall [2].

While firewalls and firewall environments are often discussed in the context of Internet connectivity, firewalls have applicability in network environments beyond Internet connectivity. For example, many corporate enterprise intranets employ firewalls to restrict connectivity to and from internal networks servicing more sensitive functions, such as the accounting or personnel department. By employing firewalls to control

Copyright © 2015 IJISM, All right reserved

connectivity to these areas, an organization can prevent unauthorized access to the respective systems and resources within the more sensitive areas. The inclusion of an internal firewall environment can therefore provide an additional layer of security that would not otherwise be available.

Although firewalls afford protection of certain resources within an organization, there are some threats that firewalls cannot protect against: connections that bypass the firewall, new threats that have not yet been identified, and viruses that have been injected into the internal network. It is important to remember these shortcomings because considerations will have to be made in addition to the firewall in order to counter these additional threats and provide a more comprehensive security solution.

The following technological support represents the defensive strategies that secure department and corporate zones to offer the constituents more opportunities for protecting critical assets and services.

b. Technological Support

The authors in [2] describe eight kinds of firewall platforms: packet filter firewalls, stateful inspection firewalls, application proxy gateway firewalls, dedicated proxy firewalls, hybrid firewall technologies, network address translation, host based firewalls, and personal firewalls/personal firewall appliances.

Packet Filter Firewalls. The most basic firewall is called a packet filter. Packet filter firewalls are routing devices that include access control functionality for system addresses and communication sessions. The access control functionality of a packet filter firewall is governed by a set of directives collectively referred to as a ruleset.

Packet filter firewalls have two main strengths: speed and flexibility. Packet filter firewalls can be used to secure nearly any type of network communication or protocol. This simplicity allows packet filter firewalls to be deployed into nearly any enterprise network infrastructure. Note that their speed, flexibility, and capability to block denial-of-service and related attacks make them ideal for placement at the outermost boundary with an untrusted network.

Stateful Inspection Firewalls. Stateful inspection evolved from the need to accommodate certain features of the TCP/IP protocol suite. When an application uses a TCP (connection-oriented transport) to create a session with a remote host system, a port is also created on the source system. This port receives network traffic from the destination system. Packet filter firewalls must permit inbound network traffic on all return packets from the destination system for connection-oriented transport to occur. Opening this many ports creates an immense risk of intrusion by unauthorized users who may employ a variety of techniques to abuse the expected conventions. Stateful inspection firewalls solve this problem by creating a directory of outbound TCP connections, along with each session's corresponding client port. This "state table" is then used to validate any inbound traffic. The stateful inspection solution is more secure because the firewall tracks client ports individually rather than opening all inbound ports for external access.

Stateful inspection firewalls share the strengths and weaknesses of packet filter firewalls, but because of the state table implementation, stateful inspection firewalls are generally considered to be more secure than packet filter firewalls.

Stateful inspection firewalls can accommodate other network protocols in the same manner as packet filters, but the actual stateful inspection technology is relevant only to TCP/IP. For this reason, many texts classify stateful inspection firewalls as representing a superset of packet filter firewall functionality.

Application-Proxy Gateway Firewalls. Application proxy gateway firewalls provide additional protection by inserting the application in the communications path, looking like the end-point of the communications to both sides of the firewall. For example, a web-proxy receives requests for external, web access from inside the firewall and relays them to the exterior web page as though the firewall was the requesting web client. The external web page responds to the firewall and the firewall forwards the response to the inside client as though the firewall was the web server. No through TCP/IP connection is ever made from inside client to external web server.

Application-proxy gateway firewalls have numerous advantages over packet filter firewalls and stateful inspection packet filter firewalls. First, application-proxy gateway firewalls usually have more extensive logging capabilities resulting from the firewall being able to examine the entire network packet rather than only the network addresses and ports.

Another advantage is that application-proxy gateway firewalls allow security administrators to enforce whatever type of user authentication is considered appropriate for a given enterprise infrastructure. Application-proxy gateways can authenticate users directly, as opposed to packet filter firewalls and stateful inspection packet filter firewalls, which normally authenticate users based on the network layer address of the system on which they reside (i.e., source, destination, and type). Given that network layer addresses can be easily spoofed, the authentication capabilities inherent in application-proxy gateway architecture are superior to those found in packet filter or stateful inspection packet filter firewalls.

Dedicated Proxy Firewalls. Dedicated proxy servers differ from application-proxy gateway firewalls in that they retain proxy control of traffic, but they do not contain firewall capability. They are typically deployed behind traditional firewall platforms for this reason. In typical use, a main firewall might accept inbound traffic, determine which application is being targeted, and then hand off the traffic to the appropriate proxy server (e.g., an e-mail proxy server). The proxy server typically would perform filtering or logging operations on the traffic and then forward it to internal systems. A proxy server could also accept outbound traffic directly from internal systems, filter or log the traffic, and then pass it to the firewall for outbound delivery.

Hybrid Firewall Technologies. Recent advances in network infrastructure engineering and information security have resulted in a "blurring of the lines" that

Copyright © 2015 IJISM, All right reserved

differentiates the various firewall platforms discussed earlier. As a result, firewall products currently incorporate functionality from several different classifications of firewall platforms. For example, many packet filter or stateful inspection packet filter firewall vendors have implemented basic application-proxy functionality to offset some of the weaknesses associated with their firewall platform. In most cases, packet filter or stateful inspection packet filter firewall vendors implement application proxies to provide improved network traffic logging and user authentication in their firewalls. Nearly all major firewall vendors have introduced hybridization into their products in some manner; therefore it is not always a simple matter to decide which specific firewall product is the most suitable for a given application or enterprise infrastructure. Hybridization of firewall platforms makes the prepurchase product evaluation phase of a firewall project important. Supported feature sets, rather than firewall product classification, should drive the product selection.

Network Address Translation. Network address translation (NAT) technology was developed in response to two major issues in network engineering and security. Network address translation is an effective tool for "hiding" the network-addressing schema present behind a firewall environment. In essence, NAT allows an organization to deploy an addressing schema of its choosing behind a firewall, while still maintaining an ability to connect to external resources through the firewall. Network address translation is accomplished by one of three methods: static, hiding, and port.

Host-based Firewalls. Firewall packages are available in some OSs or as add-ons; they can be used to secure only the individual host. Internal servers should be protected and should not be assumed to be safe from attack because they are behind a main firewall. Host-based firewall packages typically provide access-control capability for restricting traffic to and from servers running on the host, and logging is usually available. A disadvantage to host-based firewalls is that they must be administered separately and maintaining security becomes more difficult as the number of devices to be configured increases.

Personal Firewalls/Personal Firewall Appliances. Securing personal computers (PC) at home or remote locations is now as important as securing them at the office; many personnel telecommute or work at home and operate on organization- or agency-proprietary data. Home users dialing an Internet service provider (ISP) may have limited firewall protections available to them because the ISP has to accommodate potentially many different security policies. Therefore, personal firewalls have been developed to provide protection for remote systems and to perform many of the same functions as larger firewalls. These products are typically implemented in one of two configurations.

Centrally Managed Distributed Firewalls. The goals for host-based firewalls and personal firewalls/appliances can also be achieved using centrally managed distributed firewall products. All of these firewall types provide firewall capability in every protected computer. Centrally managed distributed firewalls are centrally controlled but locally enforced. A security administrator defines and maintains security policies, not the end-users. This places the responsibility and capability of defining security policies in the hands of a security professional who can properly lock down the target systems. A centrally managed system is scalable because each system does not have to be administered separately. A properly executed distributed firewall system includes exception logging. More advanced systems include location intelligence so that the appropriate policy is enforced depending on the context of the connection.

Centrally managed distributed firewalls can be either software- or hardware-based firewalls. Centrally managed distributed software firewalls are similar in function and features to host-based or personal firewalls, but the security policies are centrally defined and managed. Software distributed firewalls have the benefit of unified corporate oversight of firewall implementation on individual machines, however they remain vulnerable to attacks on the host operating system from the networks, as well as intentional or unintentional tampering by users logging into the system being protected. Centrally managed distributed hardware firewalls combine the filtering capability of a firewall with the connectivity capability of a traditional connection. Filtering the data on the firewall hardware rather than the host system can make this system less vulnerable than software-based distributed firewalls. Hardware distributed firewalls can be designed to be unaffected by local or network attacks via the host operating systems. Performance and throughput of a hardware system is generally higher than software systems.

5. Public Key Infrastructure Technology

a. Description

The interconnectivity of networks and the Internet support opportunities for government and business to conduct electronic transactions. To enable these paperless business activities, it is critical to assure that the auditability and legal standing of these electronic transactions are comparable to the paper formats. One method of meeting this requirement is the use of public key technologies and infrastructure [7].

The following technological support represents the defensive strategies that secure device and exterior zones to offer the constituents more opportunities for protecting critical assets and services.

b. Technological Support

Either GE or Non-GE should understand the PKI-enabled applications that it wishes to run and the products available for those applications. Once the applications to be supported have been identified and the security policies and requirements associated with them have been defined to differentiate between PKI products. The most and efficient tools for enabling organizations to conduct secure electronic transactions over PKI enabled applications and products include the following:

S/MIME. S/MIME enables secure E-mail application that can be used to sign and encrypt e-mail. The S/MIME

Copyright © 2015 IJISM, All right reserved

software uses the subscriber's PKI client to perform PKI operations with certificates and keys.

Web servers and browsers applications. Some standard applications implement the SSL/Transport Layer security (TLS) are widely implemented and support not only PKI-based cryptographic authentication of servers and clients but also encryption of traffic in secure sessions. Again, the application either relies on a PKI vendor's PKI client or uses a built-in PKI client to perform PKI operations.

Document-signing applications. Such applications that are used with forms, document management, or workflow products to allow signatures and approvals on electronic documents and to replace signed paper documents.

Access control. The certificates are used to authenticate an identity or privilege for use in access control, and may implement single sign-on for a variety or services.

Products with built-in PKI-enabled access control. Some products that often rely on the SSL/TLS protocol uses built-in PKI-enabled access control such as firewalls, mail servers, or directory servers.

File encryption systems. Systems that may use public key certificates to manage file encryption keys and to provide for a key recovery capability, if keys are otherwise lost.

6. Malicious Code Protection Technology

a. Description

Viruses, worms and other malicious code are typically hidden in software and require a host to replicate. Malicious code protection requires strict procedures and multiple layers of defense. Protection includes prevention, detection, containment, and recovery. Protection hardware and access-control software can inhibit this code as it attempts to spread. Most security products for detecting malicious code include several programs that use different techniques.

The following technological support represents the defensive strategies that secure device zone to offer the constituents more opportunities for protecting critical assets and services.

b. Technological Support

Scanners. Scanners provide precise identification of known malicious code. Scanners search for "signature strings" or use algorithmic detection methods to identify known code. Scanners rely on a significant amount of a prior knowledge about the code. Therefore, it is critical that the signature information for scanners is current. Most scanners can be configured to automatically update their signatures from a designated source, typically on a weekly basis; scanners can also be forced to update their signatures on demand.

Integrity Checkers. Integrity checkers detect infections by searching a program or other executable code to determine if it has been altered or changed. Integrity checkers can only flag a change as suspicious; they cannot determine if the change is a genuine virus infection. These programs are usually checksum based. The integrity checking process begins with the creation of a baseline, where checksums for clean executable are computed and saved. Each time the integrity checker is run, it again makes a checksum computation and compares the result with the stored value. Note that several different kinds of checksums are used. Simple checksums are easy to defeat; cyclical redundancy checks (CRC) are better, but can still be defeated. Cryptographic checksums such as SHA provide the highest level of security.

Vulnerability Monitors. These monitors are designed to prevent modification or access to particularly sensitive parts of the system; consequently, the monitors may block an attack on those parts. This requires considerable information about "normal" system use because PC viruses typically take advantage of system vulnerabilities and do not circumvent any security features. This type of software also requires decisions from the user about permitted operations.

Behavior Blockers. These programs contain a list of rules that a legitimate program must follow. If the program breaks one of the rules, the behavior blockers alert the users. The "sandbox" concept is that untrusted code is first checked for improper behavior. If none is found, it can be run in a restricted environment, where dynamic checks are performed on each potentially dangerous action before it is permitted to take effect. By adding multiple layers of reviews and checks to the execution process, behavior blockers can prevent malicious code from performing undesirable actions.

7. Vulnerability Scanners Technology

a. Description

Vulnerability scanners examine hosts such as servers, workstations, firewalls and routers for known vulnerabilities. Each vulnerability presents a potential opportunity for attackers to gain unauthorized access to data or other system resources. Vulnerability scanners contain a database of vulnerability information, which is used to detect vulnerabilities so that administrators can mitigate through network, host and application-level measures before they are exploited. By running scanners on a regular basis, administrators can also see how effectively they have mitigated vulnerabilities that were previously identified. Products use dozens of techniques to detect vulnerabilities in hosts' operating systems, services and applications [8].

The following technological support represents the defensive strategies that secure device and corporate zones to offer the constituents more opportunities for protecting critical assets and services.

b. Technological Support

Network Vulnerability Scanners. Network vulnerability scanners are utilized to detect vulnerabilities on remote hosts by performing scans across networks. These scanners typically identify only those vulnerabilities that can be exploited remotely. Most network vulnerability scanners first perform network mapping to enumerate the hosts, then send additional scans and probes to each host to fingerprint its operating system and identify the applications and services it is running. The final step is to examine each application and service for known vulnerabilities. Some tools take this a step farther and actually attempt to validate the identified vulnerabilities by exploiting them; this is known as penetration testing.

Copyright © 2015 IJISM, All right reserved

Host Vulnerability Scanners. Host vulnerability scanners are run on a particular host to detect its vulnerabilities. These scanners identify vulnerabilities that can be exploited either remotely or locally. Typically the administrator defines security policy settings for each operating system in use, and the scanner compares the policies to the actual settings of each host. Host vulnerability scanners usually identify vulnerabilities primarily by checking configuration settings and user and group-related information, including permissions and ownership.

Outsourced Scanning. An alternative to acquiring vulnerability scanning is to contract with an outside vendor to perform the scanning. An outside vendor uses the same host and network scanners that individual organizations may have, but the vendors can typically possess a wide range of open source and commercial products, a deep knowledge of vulnerabilities and scanning techniques, and more experience in performing vulnerability scans, increasing the likelihood of detecting vulnerabilities. On the other hand, the vendors typically lack the specific knowledge of an organization's environment that is needed to determine the significance of vulnerabilities. Outsourced scanning works best when the security, network and system administrators within an organization collaborate with the vendor. Outsourced scanning is also often extended into a full penetration test to determine not only what vulnerabilities exist within an environment, but how attackers may exploit them.

IV. Incident Handling Tools

Incident handling systems can comprise group of tools that are available for both Windows and UNIX systems.

V. User Awareness and Training

GE and Non-GE users should be made aware of policies and procedures about proper use of networks, systems, and applications. Training courses about previous incidents and appropriate security countermeasures across operational, network, and host functionality of GE and Non-GE entities should also be shared with users so they can see how their actions could affect the organization. Improving user awareness regarding incidents should reduce the frequency of incidents. IT staff should be trained so that they can maintain their networks, systems, and applications in accordance with the organization's security standards

VI. Conclusion

We conclude that proposed layered cyber-security systems architecture will assist the organizations in creating clear boundaries that effectively and practically apply multiple layers of defenses.

The boundaries are conducted through proposing four zones segment information architecture for securing the main assets and services of GE and Non-GE entities in Kuwait. That are: exterior, corporate, department, and end device zone.

In each of these zones specific and unique security focus are addressed through use technological security elements. These elements are categorized into six groups which are identification and authentication, access control intrusion detection, firewall, malicious code protection, public Key-Infrastructure, and Vulnerability Scanners.

In summary, such cyber-security architecture, supporting the incident analyst with incident handling tools, and users with awareness of policies and procedures about proper use of the organization assets will assist in effectively protect GE and Non-GE entities from cyber-attacks through supporting secure operational, network, and host with safe functionality.

References

[1] Bidgoli, Hossein. "Handbook of Information Security, Volume 3: Threats, Vulnerabilities, Prevention Detection and Management." (2005).
[2] NIST SP 800-41, Guidelines on Firewalls and Firewall Policy. January 2002.
[3] NIST SP 800-53, Recommended Security Controls for Federal Information Systems, draft.
[4] NIST SP 800-64, Security Considerations in the Information System Development Life Cycle, October 2003.
[5] NIST SP 800-31, Intrusion Detection Systems. August 2001.
[6] NIST SP 800-30, Risk Management Guide for Information Technology Systems, January 2002.
[7] NIST SP 800-32, Introduction to Public Key Technology and the Federal PKI Infrastructure. February 2001.
[8] NIST SP 800-36 Guide to Selecting Information Technology Security Products, October 2003
[9] Gartner Group. Biometrics-Based Recognition for Financial Services, Context Overview Report. December 31, 1998.
[10] NIST, SP 800-70 Revision 2, Security Configuration Checklists Program for IT Products
[11] ISA-TR99.03.01: Security Technologies for Industrial Automation and Control Systems, ISA, 2007.
[12] Idaho National Laboratory, Control Systems Cyber Security: Defense in Depth Strategies, Homeland Security External Report # INL/EXT-06-11478, May 2006.
[13] Hash, Joan, et al., NIST SP 800-65, Integrating IT Security into the Capital Planning and Investment Control Process, 2005.
[14] Burr, William, et al., NIST SP 800-63, Revision 1, Electronic Authentication Guideline, 2011.
[15] Grance, Tim, et al., NIST SP 800-61, Revision 2, Computer Security Incident Handling Guide, 2012.
[16] Souppaya, Murugiah, Kent, Karen, NIST SP 800-92, Guide to Computer Security Log Management, 2006.

Copyright © 2015 IJISM, All right reserved